

去中心化公钥基础设施综述

史晔铭^{1,2}, 闫峥^{1,2}, 张滋炯^{1,2}, 王海光³, 李铁岩³

(1. 西安电子科技大学网络与信息安全学院, 陕西 西安 710126;

2. 西安电子科技大学空天地一体化综合业务网全国重点实验室, 陕西 西安 710071;

3. 华为技术有限公司可信技术实验室谢尔德实验室, 新加坡 238895)

摘要: 公钥基础设施作为网络与信息安全领域的重要组成部分, 在数字身份认证、安全数据传输和完整性保护等场景发挥着关键作用。然而, 传统公钥基础设施的中心化架构存在显著缺陷: 用户完全依赖可信第三方机构, 导致个人数据控制权被削弱, 并引发单点故障、隐私泄露、中间人攻击等系统性风险, 难以满足分布式网络环境的安全需求。为解决上述问题, 去中心化公钥基础设施利用区块链技术实现去中心化的信任分布, 有效消除单点故障风险; 分布式账本技术使用户在进行身份验证时无须暴露过多的身份信息, 降低隐私泄露的风险, 同时其公开透明与不可篡改性可抵御数据窃取与身份伪造攻击, 从而全面提升系统安全性与可靠性。系统梳理去中心化公钥基础设施的核心理论和技术基础, 继而基于网络拓扑结构和信任管理模式, 构建一个全面且系统的去中心化公钥基础设施分类框架。提出涵盖安全性、隐私性、性能以及其他维度的一系列评估指标, 并根据提出的评估指标对现有的去中心化公钥基础设施方法进行回顾和分析。总结现有的去中心化公钥基础设施方法所面临的问题, 并对未来趋势与研究方向进行展望。

关键词: 去中心化公钥基础设施; 公钥证书; 区块链; 信任管理

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2025064

Survey of decentralized public key infrastructure

SHI Chaoming^{1,2}, YAN Zheng^{1,2}, ZHANG Zitong^{1,2}, WANG Haiguang³, LI Tieyan³

1. School of Cyber Engineering, Xidian University, Xi'an 710126, China

2. State Key Laboratory of Integrated Services Network, Xidian University, Xi'an 710071, China

3. Shield Lab, Trustworthiness Lab, Huawei Technologies Co., Ltd., 238895, Singapore

Abstract: Public key infrastructure is an essential component in the field of network and information security, serving a critical role in scenarios such as digital identity authentication, secure data transmission, and integrity protection. However, the centralized architecture of traditional public key infrastructure has significant flaws, requiring users to fully rely on trusted third-party organizations, which undermines users' control over their personal data and leads to issues such as single point of failure, privacy leakage, and man-in-the-middle attack threats, thus making it difficult to adapt to the security demands of distributed network environments. To address these issues, decentralized public key infrastructure employs blockchain technology to achieve a decentralized distribution of trust, effectively eliminating the risk of single points of failure. Distributed ledger technology enables users to authenticate

收稿日期: 2025-02-12; 修回日期: 2025-06-22

通信作者: 闫峥, zyan@xidian.edu.cn

基金项目: 国家自然科学基金(U23A20300, 62072351); 陕西省自然科学基金基础研究计划重点基金(2023-JC-ZD-35)

Foundation Items: The National Natural Science Foundation of China (U23A20300, 62072351), The Key Research Project of Shaanxi Natural Science Foundation (2023-JC-ZD-35)

their identities while minimizing the exposure of personal information, thereby reducing the risk of privacy breaches. Furthermore, its transparency and immutability enhance protection against data theft and identity forgery, significantly improving the security and reliability of the system. The core theories and technological foundations of decentralized public key infrastructure are outlined. A comprehensive and systematic classification framework for decentralized public key infrastructure is constructed based on network topology and trust management models. A series of evaluation criteria encompassing security, privacy, performance, and other dimensions is proposed, and existing methods of decentralized public key infrastructure are reviewed and analyzed according to the proposed criteria. Finally, the challenges faced by current decentralized public key infrastructure methods are summarized, and insights into future trends and research directions are provided.

Keywords: decentralized public key infrastructure, digital certificate, blockchain, trust management

0 引言

随着电子交易和在线交互数量的不断增长,迫切需要设计强有力的安全机制。公钥基础设施^[1] (public key infrastructure, PKI) 作为加密通信和密钥管理的基础,已经为数字世界的安全提供了坚实的技术支撑。PKI的公钥证书将公钥绑定到特定身份(如个人、组织或设备),为在线通信、金融交易、健康医疗等领域提供了保密性、完整性和身份认证的安全框架。PKI依赖中心化的证书授权中心(certification authority, CA)来颁发、撤销和验证证书,保证通信双方通过证书相互认证并安全地交换信息,从而提供安全可靠的通信。

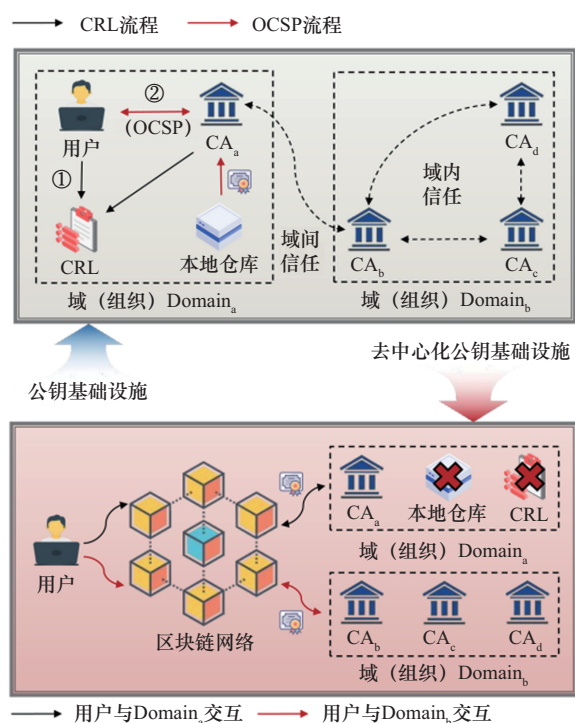
尽管PKI在数字安全领域发挥了重要作用,但其中心化架构存在显著的固有缺陷。主要体现在以下3个层面。首先,PKI依赖中心化的CA实现证书全生命周期管理,要求用户对CA节点保持绝对信任。然而,由于D2XChain外部实体无法有效验证CA内部治理机制,信任关系呈现单点脆弱性。一旦攻击者通过渗透CA节点非法签发伪造证书,即可实施中间人攻击解密通信数据,导致系统可信基石彻底崩塌。其次,PKI使用证书撤销列表^[2] (certificate revocation lists, CRL) 和在线证书状态协议^[3] (online certificate status protocol, OCSP) 查询证书的撤销状态,但这两种方法均存在验证时延高、同步周期长等缺陷,难以满足实时性要求较高的应用场景,显著降低了系统响应效率与用户体验。最后,在涉及多网络域或异构信任域的场景中,PKI需协调不同CA的信任锚点与认证策略差异。由于各域CA的信任链拓扑结构及策略实施标准缺乏互操

作性,跨域信任协商往往面临协议兼容性差、证书映射关系复杂等挑战。

为了解决上述问题,去中心化公钥基础设施(decentralized public key infrastructure, DPKI)作为新兴技术范式,近年来在学术界和工业界获得了广泛关注。DPKI通过深度融合区块链技术^[4]与密码学协议,构建了新型公钥管理体系与网络信任范式,实现了安全性增强与信任成本优化的双重目标。研究表明,DPKI在多元化应用场景中展现出显著技术价值,其核心功能主要体现在以下两个方面:一是基于分布式信任架构的身份认证机制;二是通过密码学原语为去中心化网络提供系统性的安全性与隐私性保障。在具体应用方面,Wang等^[5]针对双因素认证的安全性和可用性问题展开研究,提出了一种基于智能卡和密码组合的身份验证机制。该方案可与DPKI架构有机结合,借助分布式密钥管理机制进一步增强身份认证的去中心化特性;同时,基于密码学原语构建的DPKI系统能够有效抵御密钥泄露、重放攻击及身份伪造等安全威胁,为系统提供更可靠的安全保障。Jiang等^[6]面向云辅助自动驾驶汽车场景,提出了一种创新的统一生物识别隐私保护3因素认证(口令-生物特征-智能卡)与密钥协商协议。该方案有效解决了远程控制功能引入的安全风险,满足高安全性需求。在此场景下,DPKI可用于实现生物特征密钥的分布式存储与动态管理,其优势在于即使部分生物特征数据发生泄露,仍能确保身份认证系统的全局安全性。王菲菲等^[7]的研究聚焦于智能医疗领域,通过云计算与轻量级认证协议设计并实现了适用于智能医疗三方认证与密钥协商协议。DPKI可为此类

场景提供去中心化密钥协商方案, 在避免敏感信息暴露的同时, 维持认证协议的可验证性与审计追踪能力, 为医疗数据安全提供保障。

从图1 PKI与DPKI对比可以看出, DPKI的技术突破主要体现在以下3个方面。



首先, DPKI采用基于区块链的分布式系统构建公钥的全生命周期管理体系, 摒弃了对单一中心化CA的依赖, 有效消除了单点故障的风险。在这种分布式架构下, 区块链节点通过共识机制确保节点之间的状态同步, 单点故障不会影响整个系统的运行。其次, 相较于CRL需周期性下载撤销列表以及OCSP的在线查询时延, DPKI支持通过轻节点实时检索分布式账本, 实现证书状态秒级查询和验证, 从而显著降低了证书验证的时延。最后, 区块链还支持跨组织协同工作, 使得异构信任域间的证书互认过程无须中心化协调机构即可完成, 从而实现更高效且安全的跨组织信任体系。综上所述, DPKI克服了PKI中信任体系集中化、证书验证时延高以及跨域认证实现难等瓶颈问题, 为构建高鲁棒性的信任基础设施提供了理论范式与实践框架。

许多学者从不同角度对DPKI进行了深入调

研。Karaarslan等^[8]探讨了域名系统(domain name system, DNS)^[9]和PKI耦合体系所面临的安全性与信任问题, 揭示了DNS和CA易受到拒绝服务(denial of service, DoS)攻击^[10]、DNS欺骗^[11]、DNS缓存投毒^[12]等威胁的传导路径, 其提出的基于区块链的DNS分类框架为降低中心化风险提供了方法论支撑。Ravlija^[13]对现有的基于区块链的PKI方法进行了分类和综述, 并比较了它们在安全性、应用前景和部署成本方面的表现, 特别强调了基于区块链的PKI系统所具有的优势和面临的挑战。Brunner等^[14]对基于区块链的PKI方案进行了系统的对比分析, 总结不同方案在权限类型、存储方式、隐私保护、计算复杂度和成本等方面的特性。研究发现, 尽管现有方案基本满足PKI的核心需求, 但普遍缺乏完善的隐私保护机制, 且针对计算复杂度和成本的系统性评估不充分。De Klerk^[15]探讨了区块链在DNS和PKI中的应用, 旨在解决信任、安全和审查等问题, 特别是针对物联网(Internet of things, IoT)的挑战。该研究系统地分析了DNS和PKI的现状, 对比了区块链与非区块链方案, 并提出了一种兼具可行性和适用性的改进方法。Maldonado-Ruiz等^[16]聚焦去中心化身份管理应用, 尤其关注如何减少对可信第三方的依赖, 并指出完全去中心化的身份服务是未来值得深入探索的方向。Khan等^[17]对基于车联网的PKI(vehicular public key infrastructure, VPKI)展开了全面的调研工作, 建立的VPKI评估指标体系为特定领域DPKI设计提供参考模型。该研究重点分析了VPKI在协同智能交通系统中的应用, 特别是在证书的管理与撤销方面的挑战, 并针对未来的研究方向提出了建议, 尤其关注在高隐私与安全要求下提升系统的性能与可扩展性。Karthi^[18]开创性地探讨了智能合约与量子安全^[19]DPKI中的协同机制, 分析了基于X.509的公钥基础设施(public key infrastructure X.509, PKIX)方法存在中心化的问题。尽管现有研究在信任与安全性方面具有一定优势, 但在可扩展性、量子安全性及证书撤销机制等方面仍面临诸多挑战。Khan等^[20]针对PKIX及其证书撤销机制进行了调研, 介绍了PKIX架构及相关证书签发过程, 并分析了潜在的网络攻

击风险。随后基于系列评估指标对主流方法进行了分析与对比,探讨了如何利用区块链技术提升系统的透明性与安全性,并总结了现有工作在安全性、隐私保护及可扩展性方面的挑战与未来研究方向。本文与现有调研工作的对比见表1。从中可以看出,大多数研究缺乏细粒度的评估指标,部分研究未对DPKI方法进行详细分类。此外,现有研究对DPKI面临的潜在攻击风险的分析较为有限。尽管大部分研究在文献回顾中提及了X.509标准,但均未在X.DPKI标准的基础上进行深入分析与总结。文献[17]与文献[20]提供的调研结果相对全面。然而,前者仅聚焦于车联网的DPKI方法,其分类与评估指标难以广泛用于其他应用场景;后者虽然对PKI方法进行了深入研究,但对DPKI的分析不够全面,未能充分探讨其具体实现及应用前景。

本文系统性地梳理了DPKI领域的关键技术进展与应用实践。首先,采用形式化方法对DPKI的基本概念与框架进行理论阐述,建立统一的形式化描述体系。其次,基于信任分布特征构建了多维分类体系,从拓扑结构、共识机制和信任模型等维度对现有DPKI方案进行分析。在此基础上,本文创新性地提出了涵盖安全性、隐私保护与性能效率3个维度的综合评估指标体系,并据此对主流DPKI方法进行系统性评述,深入揭示其技术优势与实施局限。最后,归纳总结当前DPKI领域面临的关键科学问题与技术挑战,探讨了技术演进趋势与突破方向,为DPKI

体系的理论创新与工程实践提供了系统性参考框架。

1 背景知识

本节介绍与DPKI密切相关的背景知识与关键技术,并对这些核心概念和技术的深入剖析,为理解DPKI的创新价值提供了理论基础。

1.1 公钥证书

公钥证书作为数字身份认证体系的核心载体,通过密码学技术实现网络实体身份的可验证性绑定与安全通信保障。这些证书由可信的CA使用其私钥进行签署,以确保证书的有效性和可信性。在安全通信场景中,发送方使用接收方的公钥加密数据,只有持有对应私钥的接收方才能解密信息。证书签发体系采用分层架构:根CA作为信任锚点,通过逐级证书签发形成可溯源的信任链。接收方验证证书时需递归验证签发路径直至根证书,从而实现信任传递与验证。

X.509是国际电信联盟(ITU-T)于1988年首次发布的国际标准,该标准结构化公钥证书格式^[21]与认证路径验证规则,其公钥证书的组成说明见表2。如今,X.509证书已被广泛应用于如传输层安全协议(TLS)/安全套接层协议(SSL)在内的众多网络协议中,同时也用于许多非在线应用场景,如电子签名服务。X.509标准在V3版本的公钥证书中引入扩展字段,并定义包含版本号、序列号、签名算法、CA/证书主

表 1 本文与现有调研工作的对比

文献	评估指标			系统分类	协议与标准		开放性问题	未来研究方向
	安全	隐私	性能		X.509	X.DPKI		
[8]	×	×	×	√	×	×	×	×
[13]	×	×	×	√	×	×	√	×
[14]	×	×	×	×	×	×	√	×
[15]	×	×	×	×	×	×	√	√
[16]	×	×	×	×	×	×	×	√
[17]	√	√	√	√	√	×	√	√
[18]	×	×	×	×	√	×	√	√
[20]	√	√	×	×	√	×	√	√
本文	√	√	√	√	√	√	√	√

注:√表示在文献中讨论,×表示在文献中未讨论。

体唯一标识符等在内的层级化数据结构，从而成为验证实体身份的主要工具。目前，X.509标准已被 TLS/SSL/协议^[22-23]（RFC 8446）、数字签名^[24]（RFC 5652）等主流安全协议采纳，成为现代网络安全体系的基石。

表2 X.509标准公钥证书的组成说明

字段名称	说明
版本号	标识证书标准的版本（V1、V2 和 V3）
序列号	CA 分配的唯一编号，用于标识该证书
签名算法	标识用于签名证书的加密算法
签发者信息	CA 信息，由哪个机构签发的证书
有效期	证书的起始和结束有效日期
主体信息	证书持有者的信息
公钥	与证书持有者相关联的公钥
扩展字段（V3 扩展）	V3 版本的证书允许添加额外的扩展信息

1.2 信任网络

在PKI中，证书认证和验证是建立信任的基础。PKI依赖于可信的中心化CA签发和管理证书，这可能导致单点故障和信任滥用的问题。与之不同，DPKI利用公开透明、不可篡改的区块链构建信任，由区块链网络节点共同维护信任关系，进行信任决策。这种方法不仅提高了系统的韧性和安全性，同时还增强了系统的可信性，因为没有任何单一实体可以控制或操纵系统的信任关系。

信任网络（web of trust, WoT）^[25]的概念提出，旨在通过用户之间的相互认证和信任来建立一个去中心化的公钥验证系统。在该体系中，每个用户独立生成并管理自己的公钥，其他用户则通过线下或可信渠道对公钥进行验证，并将验证结果（即信任声明）以数字签名的形式进行记录。这些经过认证的信任关系可被记录并公开发布在区块链上，随着参与用户的增加和相互认证的扩展，逐步形成一个去中心化的信任网络。在信任网络的运行机制中，信任度通过多路径累积的方式建立。具体而言，当用户的公钥被多次签署和验证后，其可信度将呈递增趋势。当需要验证特定公钥的可信度时，系统可通过分析信任网络中的认证路径进行计算。这种基于社交信任的

分布式验证机制，为去中心化身份认证提供了解决方案。

1.3 CONIKS

CONIKS^[26]作为一种公钥管理方案，最初设计用于即时通信和电子邮件等应用场景，其核心目标是提供用户友好的公钥自主管理与验证机制。CONIKS采用透明日志技术实现公钥操作的全程记录与验证，其中所有公钥的注册和更新操作均被完整记录，并支持用户进行实时审计和验证，从而确保公钥信息的完整性与不可篡改性。从技术实现层面来看，透明日志基于默克尔树^[27]的数据结构构建，每个公钥操作都会生成一个包含公钥信息和操作加密证明的默克尔树叶节点。系统通过定期发布透明日志的根哈希值，为用户提供了一种高效的公钥验证机制。用户可通过验证自身公钥对应的默克尔证明，确认其公钥信息是否被正确记录。这种设计确保了所有公钥操作记录的不可篡改性，任何对公钥信息的篡改或删除操作均可通过默克尔证明被检测和识别，从而有效维护了系统的安全性和可信度。

1.4 DPKI发展历程

DPKI的技术演进与区块链、自我主权身份等技术形成协同发展态势，持续驱动数字身份管理与信任体系的结构性变革。其发展历程如图2所示。

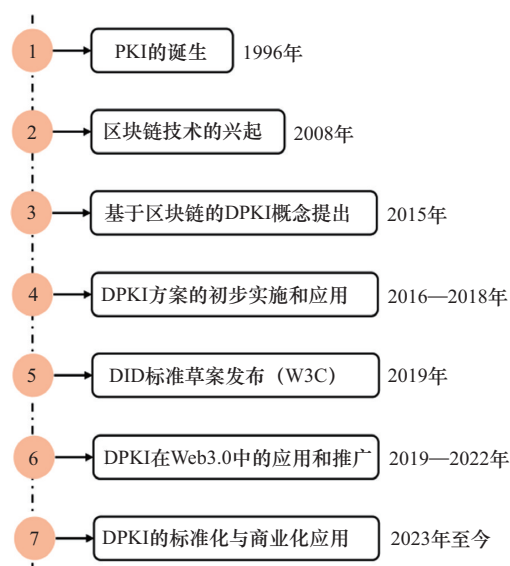


图2 去中心化公钥基础设施的发展历程

20 世纪 90 年代, 公钥基础设施体系初步建立, 通过中心化 CA 实现证书签发与公钥管理, 为网络空间身份验证与数据加密提供基础支撑; 2008 年, 区块链技术的诞生促使学术界对去中心化信任机制重构进行系统性探索, 分布式网络身份管理需求的激增推动基于区块链的 DPKI 架构^[28]理论框架成型, 研究聚焦于利用链上存储与验证机制替代中心化 CA 体系。随后 Reed 等^[29]、Lundkvist 等^[30]等相继推出原型系统。其中 Reed 提出自我主权身份^[31]的概念, Lundkvist 首先实现用户对身份数据的全生命周期自主管控。2019 年, 万维网联盟发布去中心化标识符 (decentralized identifier, DID) 标准草案^[32], 确立去中心化标识符的标准化技术框架, 促进 DID 协议在分布式身份系统中的规模化部署。随着 Web3.0 技术范式的演进, DPKI 与去中心化系统^[33]深度融合, 有效支撑 Web3.0 生态中的去中心化身份认证与隐私数据保护需求。如今, 政务机构与行业实体已在金融交易、医疗数据管理、供应链溯源等关键领域开展 DPKI 解决方案部署, 行业标准体系已经初步构建。

2 DPKI 分类

在现有的网络架构中, 中心化网络、分布式网络和去中心化网络分别代表了 3 种不同的拓扑结构与信任模型。

中心化网络中, 数据存储与控制决策高度集中于单一中心化服务器节点, 该节点承载全部计算资源分配、元数据管理及访问控制功能。网络终端节点呈星型拓扑依赖关系, 中心节点的单点故障将导致系统性服务中断。

分布式网络中, 多个半自治实体通过预设的协调机制实现资源共享与任务协同, 尽管数据副本具备多节点存储特性, 但网络仍依赖权威认证节点维持状态一致性。

去中心化网络中, 所有操作和决策都由网络节点共同协作完成, 每个节点都是平等且独立的, 没有任何一个节点完全可信并具备绝对的控制权。这种网络结构强调通过共识机制达成一致, 避免了单一节点对网络的控制, 使网络更加灵活和具有弹性。

结合网络结构, 从信任管理^[34]的角度出发, 依据用户在网络中建立和维护信任的方式, 本文提出了 DPKI 分类, 如图 3 所示。首先, 将现有的 DPKI 方法划分为两类: 混合信任模型和去中心化信任模型, 相关描述如下。

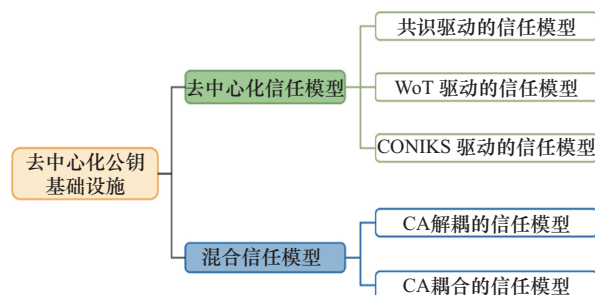


图 3 去中心化公钥基础设施分类

混合信任模型: 多个 CA 组成一个分布式网络, 用户依赖这些 CA 建立信任关系, CA 负责公钥或证书的管理及身份认证。

去中心化信任模型: 所有用户组成去中心化的自组织网络, 用户通过去中心化机制建立和维护信任关系, 无须依赖传统的 CA 机构。

在混合信任模型中, 根据区块链节点与 CA 之间的关联关系, 将混合信任模型进一步细分为 CA 解耦的信任模型和 CA 耦合的信任模型。

CA 解耦的信任模型: 信任关系由多个分布式的 CA 协同管理, CA 不直接参与区块链的共识机制, 也无须成为区块链节点。这些 CA 仍承担 PKI 中的职责, 负责证书的签发与管理。不同的是, CA 签发的证书以及证书操作均被记录在区块链中, 用户可以通过区块链账本查询证书的状态。因此, 在该模型中, 区块链仅作为透明化的工具。

CA 耦合的信任模型: CA 的功能被分散到多个区块链节点, 各节点共同承担证书的颁发和验证任务。CA 不仅负责证书颁发与管理职责, 还参与区块链的共识过程, 对其他 CA 的操作进行记录、验证和审计。

在去中心化信任模型中, 根据去中心化信任的不同实现方式将去中心化信任模型进一步分为共识驱动的信任模型、WoT 驱动的信任模型和 CONIKS 驱动的信任模型。

共识驱动的信任模型：信任关系由网络节点通过区块链的共识机制构建，所有节点共同决定哪些证书或身份是可信的。

WoT驱动的信任模型：信任由用户间信任链构建，用户通过相互签署证书表达信任，并基于这些信任链验证其他用户的证书。

CONIKS驱动的信任模型：用户的公钥或证书被记录在透明日志中，而透明日志的元数据则存储在区块链上。用户可以随时下载区块链副本，以检查证书的撤销状态。

3 评估指标

基于国际标准的规范要求与领域权威研究的评估框架^[35-36]，本节设计了一种面向去中心化公钥基础设施的多维度评估模型。如图4所示，该模型由安全性指标、隐私指标、性能指标、可用性指标及其他指标构成多维评价体系。

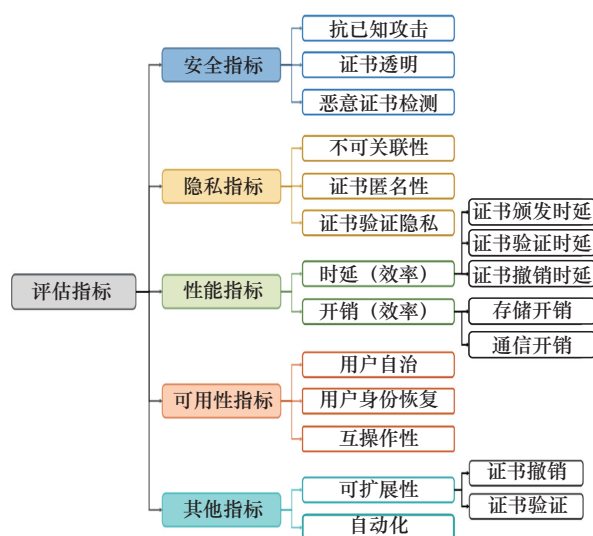


图4 去中心化公钥基础设施评估指标

3.1 安全指标

(1) 抗已知攻击

抗已知攻击^[36]指通过技术手段、协议设计及分布式机制，确保系统能够抵御已被广泛识别的攻击类型。常见的攻击类型包括DoS攻击、重放攻击^[37]、共谋攻击。DPKI中攻击面更为广泛，需要抵御针对CA节点、用户及其密钥的特定攻击，包括CA妥协攻击、女巫攻击、中间人攻击^[38]（man-in-the-middle attack, MitM）、密钥泄露攻击。针对区块链的51%攻击、智能合约漏

洞攻击等类型^[39]不属于本文的研究范畴。

(2) 证书透明

证书透明^[40]指的是证书和证书的操作日志以公开透明的方式存储在一个或多个日志中，用户可以访问这些日志来验证证书的有效性。通过对证书整个生命周期的公开透明监控和审计，使得证书的相关操作（如颁发、更新、撤销等）变得可追溯和可验证，用户能够及时发现潜在的错误或CA的不当行为。

(3) 恶意证书检测

恶意证书检测指的是通过智能方法（自动化分析或机器学习）主动检测和识别证书的恶意或异常行为，尤其是针对那些虚假但有效的证书。这种安全检测机制能够及时识别潜在的安全威胁，对恶意行为做出快速有效的响应，从而提高系统整体的安全性。

3.2 隐私指标

(1) 不可关联性

不可关联性^[41]指的是用户在不同交互或交易中使用不同的标识符或密钥，使得外部观察者无法通过这些交互数据推断出它们属于同一用户，从而保护用户隐私并防止行为被追踪或关联。在DPKI中，通常需要确保证书主体与证书交易之间具有不可关联性，以增强证书主体信息的隐私保护。具体而言，这一特性要求外部观察者无法通过分析多个不同的证书操作或交易，推断出这些操作或交易源自同一证书持有者。不可关联性指标能有效防止第三方通过观察或分析证书的使用情况来推断用户的身份或行为模式。

(2) 证书验证隐私

证书验证隐私^[20]指的是在验证证书时，用户验证信息和请求记录始终保持私密。在PKI中，用户向OCSP服务器请求证书验证时，可能暴露其正在访问的网站或服务，这可能使第三方通过分析验证请求信息来推断用户的身份信息或行为活动。

(3) 证书匿名性

匿名性是指在网络通信或数据交换过程中，用户的身份信息不会被泄露或追踪。在PKI中，用户身份往往与公钥绑定，难以实现真正的匿名。

为保护用户的身份信息，证书匿名性通过加密或匿名技术（零知识证明、环签名）保护证书持有者身份隐私的数字凭证，使得证书持有者在证书服务过程中能够始终保持匿名。同时，匿名证书的认证过程应具备足够的安全性和有效性，确保合法的证书以绝对的概率被正确验证。图 5 给出了证书验证隐私与匿名性示意。

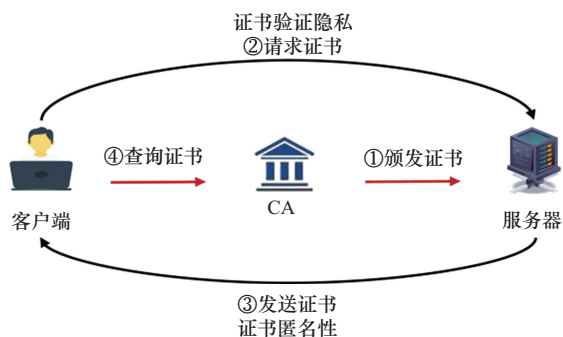


图 5 证书验证隐私与匿名性示意

3.3 性能指标

性能指标包括时延、存储开销和通信开销 3 个方面。其中，时延指的是从证书相关操作请求发出到完成的时延，涵盖证书颁发、验证和撤销操作的响应时间。存储开销指的是区块链节点或客户端存储证书及证书相关内容所需的成本。通信开销是指通信双方在执行与证书相关的操作时所产生的开销。一个高效的 DPKI 方案应能够在较短时间内处理大量的证书相关操作，并支持高并发请求处理，从而确保用户体验和系统性能的稳定。

3.4 可用性指标

（1）用户自治

用户自治^[20]指的是用户对其数字身份拥有完全的控制权，能够独立发布和管理密钥或证书。在 DPKI 方案中，用户应被允许自主生成和管理身份凭证或证书，无须依赖任何第三方的授权或控制。该指标保证了用户对其身份信息的管理具有完全的自主权，同时也加强了隐私保护。

（2）用户身份恢复

用户身份恢复^[35]指的是在身份验证令牌丢失或访问凭据遗忘的情况下，用户能够通过预设的安全机制重新获取身份验证能力的技术特

性。在 DPKI 中，身份恢复机制具体表现为：当用户私钥丢失或遭到窃取时，系统通过证书重颁发、密钥备份恢复或分片密钥重组等预置方案，协助用户重新获得对证书及相关资源的访问权限。

（3）互操作性

互操作性^[20]指的是 DPKI 方案能够在不对现有的 PKI 协议和通信协议做任何修改的情况下，无缝集成到当前的网络环境中。在 DPKI 方案中，通过与已有的标准或协议（如 X.509 标准、TLS/SSL 协议）完全兼容，使得用户和服务提供者能够在不更改底层基础设施的前提下，实现新的去中心化公钥基础设施的部署和使用，确保了 DPKI 的推广不会影响现有系统。

3.5 可用性指标

（1）可扩展性

可扩展性^[42]指的是系统在用户规模、数据体量或交易频率等负载指标持续增长的情况下，通过动态扩展计算资源、存储容量或网络带宽等基础设施，维持或提升系统性能的能力。在 DPKI 中，可扩展性主要体现在证书签发、验证与撤销等核心操作能够随证书规模的指数级增长保持稳定的处理效率。现有 DPKI 方案通过优化证书链验证算法和证书管理方法，确保系统在大规模部署时实现低时延、高吞吐量和可控的资源开销。

（2）自动化

自动化指的是 DPKI 方案是否具备自动化执行日常管理任务和支持智能化决策的能力，以减少人工干预，提高操作效率和安全性。一个方案满足该指标的条件是，使用自动证书管理环境^[43]（automatic certificate management environment, ACME）自动化地处理证书颁发、更新、撤销等操作，以确保证书生命周期管理的高效和准确，减少人工错误和操作时延。

4 文献综述

本节系统性地回顾和评述 DPKI 领域的主要研究成果与方法创新。运用安全性、隐私性、性能等评估指标，对各类方法的优势与局限性进行对比分析，结果见表 3。

表3 现有DPKI方案的评估和对比

性能	共识驱动的信任模型			WoT驱动的信任模型			CONIKS驱动的信任模型			CA解耦的信任模型			CA耦合的信任模型		
	文献[44]	文献[45]	文献[46]	文献[48]	文献[49]	文献[51]	文献[53]	文献[54]	文献[55]	文献[56]	文献[57]	文献[58]	文献[60]	文献[62]	文献[65]
鲁棒性	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
恶意证书检测	×	—	—	—	×	×	×	×	×	×	×	×	×	×	×
证书透明	√	—	—	—	√	√	√	×	√	×	×	×	√	√	√
不可关联性	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
证书匿名性	×	—	—	—	×	×	×	×	×	×	×	×	×	×	×
证书验证隐私	√	—	—	—	√	×	√	√	√	×	×	×	×	√	×
颁发时延	—	—	—	—	—	—	—	—	—	—	0.009	23.2	—	0.33	—
验证时延	9.86	—	—	—	—	—	—	6.4/13.6	19.8	—	—	28.56	—	50	—
撤销时延	—	—	—	—	—	—	—	—	—	—	—	23.3	—	—	—
通信开销	—	—	—	—	—	35 MB+ 600 B+ 80 B×N	0.5 kB×N	—	14 kB×C	—	—	3.41 kB×C	—	13 kB×C~ 73 kB×C	—
存储开销	1.93 kB×D+ 6.4 MB×N	—	—	—	1 kB×N+ 4 kB×C	80 B× (N+100)	—	—	128 kB×N	—	—	2.6 kB×N+ (127+ 0.56 kB×N (1.8 kB+ 0.42) ×C	—	—	—
用户自治	√	√	√	√	√	√	√	×	×	×	×	×	×	×	×
用户身份恢复	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
交互性	√	×	×	×	√	×	×	×	×	√	√	√	√	√	√
证书验证	×	—	—	—	×	×	√	×	×	×	×	×	√	×	—
证书撤销	×	—	—	—	×	×	×	×	×	×	×	√	√	√	—
自动化	×	—	—	—	×	×	×	×	×	×	×	×	×	×	×

注：○表示部分满足指标；√表示满足指标；×表示不满足指标；—表示未提及该指标；D表示DNS域名数量；N表示区块数量；C表示证书数量；s表示证书大小。

4.1 去中心化信任模型

4.1.1 共识驱动的信任模型

为了增强 CA 在执行证书操作时的问责性, Wang 等^[44]提出了一种基于区块链的证书透明方案。在该方案中, 服务器将证书以交易的形式发布在区块链上, 并对交易进行签名, 以防止受损的 CA 签发虚假证书。为确保证书状态的实时更新, 每笔证书交易都设有比实际证书有效期更短的有效期, 强制要求证书持有者定期发布证书并更新撤销状态。在安全性方面, 该方案通过加密客户端与服务器间的数据传输, 有效防御了中间人攻击, 但未充分考虑其他潜在攻击类型, 因此未能完全满足抗已知攻击标准。虽然该方案实现了证书及证书操作在区块链上的公开透明存储, 符合证书透明标准, 但是外部观察者可以通过分析这些记录将用户的多个操作关联起来, 违反了不可关联性原则。此外, 该方案缺乏智能的恶意证书检测功能。客户端通过下载区块链副本来验证证书的有效性, 无须向外部的 CA 或区块链节点请求, 实现了证书验证过程的隐私。同时, 该方案支持用户自主控制证书的签发与撤销过程, 充分满足了用户自治要求。该方案与现有 PKI 体系完全兼容, 满足互操作性的标准。然而, 其余关键指标没有得到充分考虑。

Namecoin^[45]作为比特币区块链^[4]的首个分叉方案, 旨在利用区块链技术构建去中心化的域名系统, 以解决传统 DNS 系统存在的中心化控制和单点故障问题。在该系统中, 域名与公钥进行绑定, 域名所有权通过私钥控制, 确保只有私钥持有者才能发布或更新与该域名关联的公钥。所有域名信息和相关操作日志以区块链交易的形式存储, 保证了域名的所有权和操作的不可篡改性。在安全性评估方面, Namecoin 方案未充分考虑潜在的风险攻击, 因此未能满足抗已知攻击标准。就隐私保护而言, 由于系统采用公开记录用户操作的设计, 外部观察者可通过分析区块链数据推断用户操作模式, 并可能关联用户真实身份, 这严重影响了系统的不可关联性。在互操作性方面, 用户需要安装额外的插件或 DNS 解析工具才能访问域名, 这种设计限制了系统的兼容性, 导致其不符合互操作性标

准。然而, Namecoin 在用户自治方面表现出显著优势, 允许用户自主发布和管理域名, 完全实现了去中心化的域名控制。需要注意的是, 由于该方案主要面向域名管理系统, 与证书相关的评估指标并不适用。

4.1.2 WoT 驱动的信任模型

Toorani 和 Gehrmann^[46]提出了一种基于区块链的去中心化动态 PKI (decentralized dynamic PKI, DDPKI) 模型, 旨在解决 PKI 系统依赖 CA 导致的单点故障、维护成本高和安全风险高等问题。DDPKI 的核心在于实现了节点间信任关系的动态调整, 支持分布式系统中密钥的动态添加与撤销。在该模型中, 新节点的加入或现有节点公钥的撤销都需要获得足够数量的信任节点的认可, 这种机制有效确保了系统在动态环境下的安全性和操作灵活性。为进一步提升系统性能, DDPKI 引入了动态密码累加器^[47], 能够快速验证公钥的有效性及其撤销状态, 无须对整个区块链进行线性扫描, 显著提升了公钥验证的计算效率。然而, 该模型在应对潜在攻击方面的研究仍显不足, 未能满足抗已知攻击标准。DDPKI 通过共识机制允许用户自主注册公钥, 并支持随时发起公钥撤销或更新请求, 这种设计赋予了用户对其身份凭证的完全控制权, 充分满足了用户自治的要求。值得注意的是, 由于 DDPKI 移除了对 CA 和传统证书的依赖, 因此与证书相关的评估指标不再适用于该模型。

Al-bassam^[48]提出了一种基于以太坊的身份管理系统——SCPKI (smart contract-based PKI), 旨在提升 PKI 系统的透明性、安全性和去中心化程度。SCPKI 将用户身份信息 (如姓名或地址) 与公钥进行绑定, 并结合数字签名和信任网络技术, 构建去中心化的身份认证体系。该系统允许多个用户对其他用户的身份信息进行签名和背书, 从而形成分布式信任网络。然而, SCPKI 在应对潜在攻击风险方面缺乏深入考虑, 未能完全满足抗已知攻击标准。该系统摒弃了中心化的 CA, 用户能够在无须依赖单一信任实体的情况下注册、更新和撤销公钥, 充分实现了用户自治。系统通过智能合约记录用户的身份和公钥信息, 并将所有操作记录公开存储在区块链上。

这种设计虽然提高了系统透明度，但也带来了隐私风险：外部观察者可通过分析公钥操作模式，推测用户是否进行了多个相关操作，从而可能暴露用户身份，这违反了不可关联性原则。值得注意的是，由于 SCPKI 完全移除了对 CA 和传统证书的依赖，因此与证书相关的评估指标不再适用于该系统。

为了解决 PGP 密钥服务器的安全和信任问题，Yakubov 等^[49]提出了一种基于以太坊区块链的框架——BlockPGP，用于管理颇好保密性（PGP）证书^[50]和密钥服务器。该框架将以以太坊地址集成到标准化证书的注释字段中，其他用户验证该地址以及证书持有者的信息，并对证书进行签名。系统支持用户向区块链发布证书、签署其他用户证书、撤销已签名证书或自有证书等操作。与传统的 PGP 密钥服务器不同，BlockPGP 严格限制了证书管理权限，仅允许证书持有者或授权管理员发布和管理证书。在安全性方面，该框架未对潜在风险攻击进行深入研究和防护设计，因此未能满足抗已知攻击标准。虽然通过区块链和智能合约提供了对恶意证书的间接防护机制，但缺乏主动检测和防御恶意证书的有效方案。证书被同步存储在密钥服务器和区块链中，其他用户可以下载区块链副本获取证书，从而实现了证书透明。该框架允许用户自主管理其 PGP 密钥并不依赖于中心化实体，但由于所有操作均在区块链上公开且与特定密钥相关，因此外部观察者可能通过分析区块链上公开的记录推测用户行为。该方案没有考虑证书匿名性、互操作性和证书自动化管理。

4.1.3 CONIKS 驱动的信任模型

Tomescu 和 Devadas^[51]提出了一种名为 Catena 的高效、不可篡改的日志系统，该系统基于比特币区块链构建，旨在防御日志中的双重支出攻击和不一致性，特别是针对“等价攻击”^[52]。Catena 将 CONIKS 的操作日志记录在区块链中，利用比特币区块链的防御双花攻击的特性，确保日志中的声明不能被篡改或分叉。在该系统中，只有当区块链发生成功分叉时，日志服务器中的数据才可能被修改，这使得篡改日志的难度与篡改比特币区块链的难度相当，有效防御了中间人

攻击。然而，该系统主要关注区块链层面的风险攻击，未充分考虑 DPKI 系统中的潜在风险，因此未能完全满足抗已知攻击标准。Catena 可广泛应用于公共密钥目录、Tor 目录服务器和软件透明性方案等场景，完全支持证书透明标准。系统允许用户在不依赖任何中心化实体的情况下自主发布和管理证书，充分实现了用户自治。然而，系统在恶意证书检测方面存在局限，主要依赖外部用户或审计员的主动查询和验证，缺乏自动化的恶意证书检测机制。在该系统中，客户端的证书验证请求是公开的，未能实现证书验证隐私。同时，系统公开操作记录可能导致外部观察者通过分析这些记录，将用户的操作关联起来，从而未实现不可关联性。其余关键指标未得到讨论和关注。

Dong 等^[53]提出了一个名为 Conifer 的结合中心化管理和区块链的 DPKI 方案，旨在解决 PKI 系统的信任中心化和区块链的可扩展性差问题。Conifer 的核心是引入了“操作森林”数据结构，该结构由多个按时间顺序排列的操作树组成，用于详细记录每个名称在命名空间中的变更历史。其中，操作树采用默克尔二叉搜索树实现，其根哈希值被存储在区块链交易链中，确保了操作树根哈希的不可篡改性。为增强系统灵活性，Conifer 引入了身份脚本概念，允许用户通过可编程方式定义身份验证规则。然而，这种设计也带来了隐私风险：外部观察者可通过分析操作日志将特定操作与用户关联，导致系统未能达到不可关联性标准。Conifer 通过操作树的数据结构提供了高效的查找和验证机制，提升了系统的可扩展性。然而，其他指标未得到充分考虑和讨论。

4.2 混合信任模型

4.2.1 CA 解耦的信任模型

为解决 PKI 存在的 CA 妥协或故障导致的单点故障等问题，Yakubov 等^[54]提出了一个基于区块链的 PKI 管理方案。该方案利用区块链的分布式账本技术取代了传统的中心化证书透明方法，使证书的颁发和撤销过程完全公开透明。通过共识机制，所有区块链节点都能够验证证书信息的有效性。此外，框架实现了包含根 CA、子 CA

和终端用户的分层架构,支持从叶子证书到根证书的完整证书授权树(信任链)验证。然而,该方案在安全性方面存在明显不足:缺乏对潜在攻击的深入分析和防御机制设计,未能满足抗已知攻击标准;同时,未建立有效的恶意证书检测机制。在隐私保护方面,该方案未能实现任何隐私性指标,存在用户隐私泄露风险。就性能而言,由于未采用模块化设计,该方案在可扩展性方面表现欠佳。

Kubilay 等^[55]提出了一个名为 CertLedger 新颖的基于区块链的 DPKI 模型,旨在解决 PKI 系统中存在的证书验证和撤销透明度不足、隐私泄露以及客户证书验证烦琐等问题。CertLedger 将 TLS 证书的颁发、存储和撤销过程转移至区块链中,并通过自动构建并验证证书的可信路径,简化了客户端的证书验证流程。CertLedger 通过区块链防止攻击者向客户端展示不同版本的日志,避免了伪造证书的存在,有效抵御 MitM 攻击。然而,该方案对其他潜在攻击类型的讨论和防护措施仍显不足,未能完全满足抗已知攻击标准。CertLedger 虽然提供了检测伪造 TLS 证书和欺诈性撤销的基础设施,但仍依赖客户端(如浏览器)或区块链节点进行验证,缺乏自动化的恶意证书检测机制。就透明性而言,证书被存储在区块链的域状态对象中,对所有节点公开可见,完全达到了证书透明标准。然而,用户证书仍需通过中心化 CA 进行身份验证,这种设计违背了用户自治原则。此外,由于所有证书相关操作记录均公开存储,外部观察者可通过分析这些记录推断用户行为模式,导致系统未能实现不可关联性。在隐私保护方面,CertLedger 通过区块链验证证书有效性,确保了用户信息在验证过程中的安全性。同时,该系统保持了对现有 X.509 证书、TLS/SSL 协议和 CA 架构的兼容性,满足互操作性要求。然而,其他关键性能指标尚未得到充分论证和实现。

为应对现有 IoT 医疗系统在数据安全、隐私保护和密钥管理方面的技术挑战,Joseph 等^[56]提出了一种基于区块链的 PKI 解决方案。该方案利用区块链技术实现去中心化的存储与证书管理机制,有效缓解 PKI 中因依赖中心化 CA 而导致的

单点故障风险。通过部署智能合约,该方案实现了 IoT 设备的公钥注册、证书颁发、验证与撤销等全流程自动化管理,显著提升了操作透明度与审计追踪能力,同时确保了数据的完整性和访问控制安全性。该方案还集成了先进的加密算法与身份验证协议,构建了多层次的医疗数据保护体系。在安全性方面,由于缺乏针对潜在攻击的防御策略设计,方案未能满足抗已知攻击的标准要求;虽然所有证书操作均可公开验证,但证书本身的透明度不足,不符合证书透明标准;同时,该方案未建立有效的恶意证书检测机制,存在恶意证书滥用的潜在风险。在隐私保护方面,公开账本架构导致证书操作行为可被链上分析技术逆向关联,违背了不可关联性的原则。在可扩展性方面,该方案未提出适用于海量 IoT 设备场景的证书验证和撤销管理方法,难以满足大规模部署需求。就用户指标而言,虽然该方案利用智能合约实现证书的全生命周期管理,减少了对中心化 CA 的依赖,但 IoT 设备的身份注册仍需依赖 CA 节点完成,未能实现用户自治。该方案兼容现有 PKI 标准,满足互操作性要求,但其证书生命周期管理依赖人工干预,缺乏自动化证书管理方法,可能引发新的安全风险。该方案中其他指标尚未得到充分的讨论和关注。

Akram 等^[57]针对无人机物联网(Internet of drone things, IoDT)场景下中心化 CA 存在的单点故障和安全风险问题,提出了一种基于区块链的 PKI 方案——D2XChain (decentralized drone X.509 chain)。该方案通过区块链技术实现去中心化的 CA 管理,并利用智能合约自动化执行证书全生命周期操作。同时提出了服务证明(proof-of-service, PoS)共识机制,有效确保了证书操作的透明性和不可篡改性。在安全性方面,D2XChain 能够有效抵御中间人攻击,但方案设计未充分考虑其他潜在风险攻击,因此在抗已知攻击标准方面存在不足。虽然证书操作记录被存储在区块链上,但证书本身的公开透明存储机制尚未实现,未能完全满足证书透明标准。此外,尽管方案通过共识机制与智能合约实现了证书有效性验证,但在智能化恶意证书检测方法方面仍存在改进空间。D2XChain 展现出显著优势,其

完全兼容 X.509 标准, 并能够实现与现有 PKI 系统的无缝集成, 充分满足了互操作性要求。然而, 该方案在隐私保护机制和系统可扩展性方面的设计仍显不足, 其他指标尚未得到充分论证和讨论。

4.2.2 CA 耦合的信任模型

为解决现有证书管理机制中的中心化信任风险高和可验证性差的问题, Chen 等^[58]提出了基于区块链的去中心化证书审计方案——CertChain。该方案采用了基于信任评分的共识协议, 确保网络中的参与者公平参与区块生成过程。同时, 设计了一种名为 CertOper 的数据结构, 用于记录所有证书操作的历史, 从而实现高效的证书操作追溯和查询。为提升证书撤销和验证效率, 该方案引入了双计数布隆过滤器^[59] (dual counting Bloom filter, DCBF), 这不仅有效降低了假阳性的概率, 还减少了存储和计算成本。该方案未考虑 DPKI 风险攻击, 因此不满足抗已知攻击的标准。虽然证书操作日志被记录在区块链上, 但证书并未公开存储, 因此未完全实现证书透明性。虽然该方案通过区块链节点的共识机制间接实现了恶意证书检测, 但缺少智能的恶意证书检测机制。由于证书的操作记录和验证信息是公开存储在区块链上的, 潜在的恶意实体可以通过分析这些数据, 推测出特定用户的身份。此外, 用户在证书验证阶段需要向区块链节点发送包含证书信息的验证请求, 这破坏了证书验证隐私。CertChain 通过 DCBF 提高了证书撤销检查的可扩展性, 但在证书验证方面的可扩展性问题仍未得到充分讨论和解决。CertChain 依然依赖中心化 CA 进行证书签发, 因此未能满足用户自治的标准。CertChain 与现有的 X.509 标准和 TLS 协议兼容, 具有良好的互操作性。证书匿名性和自动化等指标未得到充分关注和探讨。

Qin 等^[60]提出了一个名为 Cecoin 的基于区块链的 DPKI 方案, 旨在解决 PKI 所面临的单点故障和安全性问题。Cecoin 设计了一种改进的默克尔帕特里夏树 (Merkle Patricia tree, MPT) 数据结构, 构建了去中心化的证书库, 显著提升了证书的存储与检索效率。该设计提高了证书操作 (如注册、撤销、更新和验证) 的效率和安全性。

此外, Cecoin 引入了一个在线公平交换协议^[61], 使用户在没有可信第三方参与的情况下进行身份转让, 确保了交易过程中的公平性。在安全性方面, Cecoin 通过将公钥与用户身份绑定, 有效防御了中间人攻击, 防止攻击者在通信过程中插入伪造公钥或篡改证书。然而, 由于未充分考虑其他类型的潜在攻击, 该方案未能完全满足抗已知攻击标准。就透明性而言, Cecoin 利用 MPT 数据结构存储证书及其哈希值, 完全实现了证书透明标准。系统支持用户自主发布、更新和撤销证书, 无须依赖中心化实体, 满足了用户自治要求。然而, 公开的用户操作记录可能导致外部观察者通过分析将多个操作关联到同一用户, 违反了不可关联性原则。同时, 证书状态、操作记录和验证请求等信息的公开性, 使得用户活动模式可能被推测, 破坏了证书验证隐私。尽管如此, Cecoin 通过证书库结构显著提升了证书验证和撤销操作的效率, 增强了系统的可扩展性。然而, 其他关键指标未得到充分讨论和关注。

针对 5G 服务化架构 (service-based architecture, SBA) 中因依赖中心化 CA 与网络存储功能 (network repository function, NRF) 引发的单点故障、隐私泄露及安全脆弱性问题, Fei 等^[62]提出了一种基于区块链的 5G 网络功能管理方案——B5G-NFM。该方案通过区块链中间件实现 5G 核心网与分布式账本的协议集成, 构建了去中心化的网络功能 (network function, NF) 证书管理体系; B5G-NFM 引入基于双线性配对的可撤销聚合签名算法, 将 NF 的多证书验证过程聚合为单一验签操作, 显著提升了证书管理效率。并采用智能合约驱动的星际文件系统^[63] (interplanetary file system, IPFS) 实现证书的链下存储, 有效解决了区块链场景下的数据读写性能瓶颈问题。在安全性方面, B5G-NFM 能够抵御中间人攻击、仿冒攻击、CA 妥协攻击, 但由于未考虑其他潜在风险攻击, 因此未能完全满足抗已知攻击的标准。在证书透明度方面, 方案将证书操作记录存储在区块链上, 而证书本身则加密存储在 IPFS 中, 任何节点均可通过哈希值检索证书, 符合证书透明标准。就隐私保护而言, 该方案采用模糊

传输与零知识证明的协同方法,有效保障了跨域 NF 交互时的访问令牌机密性,从而满足证书验证隐私的标准。在可扩展性设计上,B5G-NFM 通过可撤销的聚合签名算法和 FISCO BCOS^[64]多组并行机制对大规模网络的支持,显著提升了证书撤销的可扩展性。此外,该方案完全兼容 X.509 标准,支持与现有 5G SBA 的无缝集成,从而满足互操作性的标准。然而,其他指标尚未得到充分讨论。

国际电信联盟发布去中心化公钥基础设施系统架构与标准化规范 X.DPKI^[65],为公钥基础设施的革新提供了标准化框架。该标准将区块链网络与 CA 和属性机构(attribute authorities, AA)进行整合,构建去中心化的公钥基础设施体系。在该体系中,各参与节点基于拜占庭容错共识算法维护分布式账本,完整记录证书、属性证书及其全生命周期状态,从而有效消除了对单一信任锚点的依赖。X.DPKI 标准规范了 CA 与 AA 的证书注册、更新及撤销等全流程管理。X.DPKI 标准的发布标志着公钥基础设施体系从中心化架构向去中心化、高可扩展方向的范式转型,其技术创新路径可体现在以下 3 个方面首先,公钥证书与密码学技术深度耦合,将 SM2/SM3/SM4 等国密算法嵌入 DPKI 的密钥生成、数字签名及数据加密等核心模块,不仅能够满足密码自主可控的要求,还通过椭圆曲线算法的低计算开销特性,优化了分布式场景下的性能损耗。其次,针对大规模设备接入场景,DPKI 引入状态分片与交易分片双重机制:状态分片通过水平扩展构建并行子链集群,而交易分片采用批量处理降低跨片通信开销。这种分片技术将传统区块链的吞吐量从百级提升至万级,有效解决了大规模场景下的性能瓶颈问题。最后,X.DPKI 标准的发布促进了跨领域融合创新,催生了传统领域的新应用。区块链技术的引入使得证书信息的验证和更新更加透明、高效,减少了中间人攻击和证书伪造的风险,这对于金融、医疗、能源等关键基础设施的安全性至关重要。特别是在跨域信任方面,DPKI 通过区块链技术实现了全球范围内的去中心化信任机制,使得不同 PKI 域之间的信任建立更加便捷。这一特性对于全球化的企业和服

务提供商尤为重要,有助于促进跨域合作和数据共享。具体应用场景包括但不限于以下场景:在金融科技领域,构建跨机构联盟链可信交互框架,实现供应链金融场景企业数字身份链上互认;在智慧城市领域,结合隐私计算技术,支撑亿级物联网设备动态身份管理与数据最小化披露;在车联网领域,依托边缘计算节点部署分布式证书服务,满足通信的低时延认证需求。

5 开放性问题 and 未来研究方向

基于对现有 DPKI 方案的系统性综述与分析,本节将归纳总结当前 DPKI 领域面临的关键开放性问题,并以此为基础结合新兴技术发展趋势,提出未来研究方向。

5.1 恶意证书检测

(1) 开放性问题

现有研究主要依赖区块链的共识机制检测恶意证书,或通过用户举报机制识别异常行为。然而,这些方法属于被动式响应,缺乏主动、智能的分析与防御机制,尤其在伪造证书的自动化检测和防护方面存在显著不足。这种局限性可能导致攻击者能够长期利用伪造证书实施恶意操作而不被及时察觉,进而可能引发系统级的安全风险,甚至导致整个信任体系的崩溃。因此,开发基于机器学习和行为分析的主动防御机制,实现恶意证书的实时检测与自动响应,已成为提升 DPKI 系统安全性的关键研究方向。

(2) 未来研究方向

为解决现有方案在恶意证书和异常行为检测方面的智能化不足问题,未来研究可以重点探索基于机器学习的智能检测系统。具体而言,可考虑以下技术路径:首先,利用聚类算法^[65]对证书操作行为进行模式识别和异常检测,自动识别偏离正常模式的异常操作;其次,整合大语言模型^[67]的语义分析能力,实现对证书操作日志的智能解析和潜在威胁预测。通过构建自动化的证书行为分析模型,系统能够有效区分正常证书操作与潜在恶意行为,实现从被动响应到主动防御的范式转变。这种智能化检测机制不仅

能够提高恶意证书的识别准确率，还能显著缩短威胁响应时间，为DPKI系统的安全性提供有力保障。

5.2 不可关联性

(1) 开放性问题

现有研究在追求公开透明的同时，往往忽视了不可关联性的问题，导致用户信息隐私泄露^[68]。具体而言，用户的各类操作记录（包括证书颁发、更新、撤销等）均被完整记录在区块链上，这使得外部观察者能够通过高级关联分析技术，将不同操作与特定用户进行关联，进而推断出用户的身份信息或行为模式。这种隐私泄露问题可能被攻击者利用，实施针对性的攻击行为。例如，通过分析用户行为模式发起中间人攻击，或利用操作时序特征进行重放攻击。因此，如何在保证系统透明性的同时实现操作不可关联性，已成为DPKI系统设计中亟待解决的关键问题。

(2) 未来研究方向

为解决不可关联性与公开透明性之间的固有矛盾，未来研究可重点探索基于无条件匿名技术^[69]的DPKI方案。具体而言，通过环签名或群签名等密码学原语，使用户操作能够以完全匿名的方式记录在区块链上，确保外部观察者无法确定具体操作的执行者身份。此外，还可引入一次性公钥机制，即用户每次操作都生成并使用新的公钥，有效阻断基于公钥的关联分析。为进一步增强隐私保护效果，可结合交易混淆技术，通过打乱交易时序和关联关系，大幅提高外部观察者追踪用户操作的难度。这种多层次隐私保护框架能够在确保系统透明性和可验证性的同时，为用户操作提供强有力的不可关联性保障。

5.3 证书匿名性

(1) 开放性问题

现有研究在证书主体和服务器身份匿名性保护方面仍存在明显不足，导致身份信息在证书签发、使用和验证过程中面临泄露风险。具体而言，证书操作的全生命周期信息被公开记录并在系统中传播，使得攻击者能够通过分析证书使用模式推断用户身份。这一问题在跨域场景中尤为

突出：由于不同组织和系统间存在信任基础差异和协议异构性，身份信息在跨域交互过程中更容易被追踪和关联。例如，在跨组织协作或跨境业务场景中，证书持有者的身份可能通过证书使用模式、时间戳信息或网络流量特征被识别，进而导致敏感信息泄露。因此，开发支持强匿名性的跨域证书管理机制，实现身份信息与证书操作的完全解耦，已成为提升DPKI系统隐私保护能力的关键研究方向。

(2) 未来研究方向

为解决证书持有者及服务器身份泄露问题，未来研究可重点探索基于先进密码学技术的匿名证书方案。具体而言，可结合零知识证明技术，使证书持有者和服务器能够在无须暴露真实身份的情况下完成证书的签发、验证和管理等操作，从而显著增强身份隐私保护。同时，研究可整合DID技术，构建分布式的身份匿名机制。该机制允许用户在不同交互场景中实现细粒度的身份信息选择性披露，例如，仅提供必要的属性证明而非完整身份信息。这种基于DID的分布式身份管理框架特别适用于跨域场景，能够有效防止身份信息在跨组织、跨系统交互过程中的泄露和关联，为用户提供更强的隐私保护能力。此外，还可探索将同态加密、安全多方计算等隐私增强技术与匿名证书方案相结合，进一步提升系统的安全性和实用性。

5.4 可扩展性

(1) 开放性问题

现有研究在处理大规模证书验证和撤销操作时，面临显著的可扩展性挑战。首先，区块链系统要求所有节点同步完整的区块链数据，导致计算和存储开销呈指数级增长，这不仅增加了节点的硬件资源需求，还引发了数据同步时延和计算复杂度攀升的问题。其次，部分方案仍依赖传统PKI中的CRL或OCSP机制，这些机制在去中心化环境中表现出明显的效率不足：CRL的定期更新机制导致撤销信息传播时延，而OCSP的单点查询模式难以应对大规模并发请求。特别是在处理海量证书时，这些局限性更加突出，可能导致撤销信息传播滞后，给系统带来严重的安全隐患。因此，开发高效、实时的分布式证书验证和

撤销机制, 已成为提升 DPKI 系统可扩展性的关键研究方向。

(2) 未来研究方向

为应对大规模网络环境下的可扩展性挑战, 未来研究可从以下方向展开: 首先, 可探索基于区块链分片技术^[70]的创新方案, 通过将网络划分为多个并行处理的子链, 显著提升系统的交易处理能力和并行效率, 其次, 可结合链下技术^[71], 将部分证书验证和撤销操作迁移至链下执行, 仅将关键验证结果提交至主链, 从而减轻区块链的存储和计算负担。此外, 研究可致力于开发新型轻量级验证节点架构, 这些节点无须维护完整的区块链账本, 而是通过验证区块头信息或 Merkle 证明等元数据来完成交易验证, 在保证安全性的同时大幅降低资源开销。这种多层次的可扩展性优化方案能够有效提升 DPKI 系统在大规模网络环境下的性能表现, 为海量设备接入提供可靠支持。

5.5 自动化证书管理

(1) 开放性问题

现有研究在自动化证书管理机制方面仍存在明显不足, 这导致用户和系统管理员在处理大规模证书时面临严重的可扩展性问题。具体而言, 现有方案过度依赖人工干预的证书管理方式, 不仅增加了操作复杂性, 还引入了潜在的安全风险: 人为错误可能导致安全策略配置不当, 或未能及时处理失效证书。更为严重的是, 缺乏高效的自动化管理机制可能导致证书更新和撤销操作滞后, 使得已失效或存在安全漏洞的证书仍可被继续使用, 为攻击者提供了可乘之机。例如, 攻击者可能利用过期的特权证书实施横向移动攻击, 或通过未及时撤销的泄露证书发起中间人攻击。因此, 开发智能化的自动化证书管理框架, 实现证书生命周期的全流程自动化监控和管理, 已成为提升 DPKI 系统安全性和可用性的关键研究方向。

(2) 未来研究方向

为解决现有证书管理中的自动化不足问题, 未来研究可重点探索基于智能合约的 ACME^[43]。具体而言, 可设计智能合约驱动的 ACME 协议, 利用其自动化证书请求处理和验证的特性, 实

现证书颁发、更新、撤销等全生命周期管理的自动化执行。这种智能合约框架可根据预设条件(如证书到期时间、安全策略变更等)自动触发相关操作, 完全消除人工干预需求。此外, 研究可进一步整合机器学习算法, 使系统能够智能预测证书使用模式, 优化证书更新策略。ACME 的深度应用不仅能够显著降低手动证书管理的复杂性, 还将大幅提升系统的自动化水平和响应效率, 为大规模证书管理提供可靠的技术支撑。

参考文献:

- [1] MAURER U. Modelling a public-key infrastructure[C]//Computer Security—ESORICS 96. Berlin: Springer, 1996: 325-350.
- [2] NAOR M, NISSIM K. Certificate revocation and certificate update[J]. IEEE Journal on Selected Areas in Communications, 2000, 18(4): 561-570.
- [3] MYERS M, ANKNEY R, MALPANI A, et al. X. 509 Internet public key infrastructure online certificate status protocol-OCSP[R]. RFC 2560, 1999.
- [4] SQUAREPANTS S. Bitcoin: a peer-to-peer electronic cash system[J]. SSRN Electronic Journal, 2008.
- [5] WANG D, WANG P. Two birds with one stone: two-factor authentication with security beyond conventional bound[J]. IEEE Transactions on Dependable and Secure Computing, 2018, 15(4): 708-722.
- [6] JIANG Q, ZHANG N, NI J B, et al. Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles[J]. IEEE Transactions on Vehicular Technology, 2020, 69(9): 9390-9401.
- [7] 王菲菲, 汪定. 基于雾计算的智能医疗三方认证与密钥协商协议[J]. 软件学报, 2023, 34(7): 3272-3291.
WANG F F, WANG D. Fog computing-based three-party authentication and key agreement protocol for smart healthcare[J]. Journal of Software, 2023, 34(7): 3272-3291.
- [8] KARAARSLAN E, ADIGUZEL E. Blockchain based DNS and PKI solutions[J]. IEEE Communications Standards Magazine, 2018, 2(3): 52-57.
- [9] MOCKAPETRIS P, DUNLAP K J. Development of the domain name system[C]//Symposium Proceedings on Communications Architectures and Protocols. New York: ACM, 1988: 123-133.
- [10] LAU F, RUBIN S H, SMITH M H, et al. Distributed denial of service attacks[C]//Proceedings of the SMC 2000 Conference Proceedings. 2000 IEEE International Conference on Systems, Man and Cybernetics. Cybernetics Evolving to Systems, Humans, Organizations, and Their Complex Interactions. Piscataway: IEEE Press, 2000: 2275-2280.
- [11] STEINHOFF U, WIESMAIER A, ARAÚJO R. The state of the art

- in DNS spoofing[C]//Proceedings of the 4th International Conference on Applied Cryptography and Network Security (ACNS 2006). Berlin: Springer, 2006: 238-252.
- [12] SON S, SHMATIKOV V. The hitchhiker's guide to DNS cache poisoning[C]//Security and Privacy in Communication Networks. Berlin: Springer, 2010: 466-483.
- [13] RAVLIJA D. PKIs based on blockchains[D]. Stuttgart:University of Stuttgart, 2019.
- [14] BRUNNER C, KNIRSCH F, UNTERWEGER A, et al. A comparison of blockchain-based PKI implementations[C]//Proceedings of the 6th International Conference on Information Systems Security and Privacy (ICISSP 2020). Setúbal: Scitepress, 2020: 333-340.
- [15] DE KLERK L. Blockchain-based DNS and PKI to solve issues of trust, security and censorship in the context of the IoT [C]//Proceedings of the 2022 IEEE Region 10 Symposium (TENSYP). Singapore: IEEE, 2022: 1-6.
- [16] MALDONADO-RUIZ D, TORRES J, MADHOUN N, et al. Current trends in blockchain implementations on the paradigm of public key infrastructure: a survey[J]. IEEE Access, 2022, 10: 17641-17655.
- [17] KHAN S, LUO F, ZHANG Z, et al. Survey on issues and recent advances in vehicular public key infrastructure (VPKI)[J]. IEEE Communications Surveys & Tutorials, 2022, 24(3): 1574-1601.
- [18] KARTHA N. An overview of distributed public key infrastructures (DPKIs)[EB]. 2022.
- [19] PORTMANN C, RENNER R. Security in quantum cryptography [J]. Reviews of Modern Physics, 2022, 94(2): 025008.
- [20] KHAN S, LUO F, ZHANG Z J, et al. A survey on X.509 public-key infrastructure, certificate revocation, and their modern implementation on blockchain and ledger technologies[J]. IEEE Communications Surveys & Tutorials, 2023, 25(4): 2529-2568.
- [21] COOPER D, SANTESSON S, FARRELL S, et al. Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile[R]. RFC 5280, 2008.
- [22] FREIER A, KARLTON P, KOCHER P. The secure sockets layer (SSL) protocol version 3.0[R]. RFC 6101, 2011.
- [23] DIERKS T, RESCORLA E. The transport layer security (TLS) protocol version 1.2[R]. RFC 5246, 2008.
- [24] HOUSLEY R. Cryptographic message syntax[R]. RFC 2630, 1999.
- [25] ZIMMERMANN P. The official PGP user's guide[M]. Cambridge, MA: MIT Press, 1995.
- [26] MELARA M S, BLANKSTEIN A, BONNEAU J, et al. CONIKS: Bringing key transparency to end users[C]//Proceedings of the 24th USENIX Security Symposium. Washington, D C : USENIX Association, 2015: 383-398.
- [27] SZYDLO M. Merkle tree traversal in log space and time[C]//Proceedings of the Advances in Cryptology - EUROCRYPT 2004: International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2004: 541-554.
- [28] AXON L, GOLDSMITH M. PB-PKI: a privacy-aware blockchain-based PKI[C]//Proceedings of the 14th International Conference on Security and Cryptography (SECRYPT 2017). Madrid, Spain: SciTePress, 2017: 311-318.
- [29] REED D, LAW J, HARDMAN D. The technical foundations of sovryn : a white paper from the sovryn foundation[EB]. 2016.
- [30] LUNDKVIST C, HECK R, TORSTENSSON J, et al. Uport: a platform for self-sovereign identity[EB]. 2016.
- [31] MÜHLE A, GRÜNER A, GAYVORONSKAYA T, et al. A survey on essential components of a self-sovereign identity[J]. Computer Science Review, 2018, 30: 80-86.
- [32] REED D, SPURNY M, LONGLEY D, et al. Decentralized identifiers (DIDs) v1.0[S]. W3C Recommendation, 2020.
- [33] ZHENG Z B, XIE S A, DAI H N, et al. An overview of blockchain technology: architecture, consensus, and future trends[C]//Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress). Piscataway: IEEE Press, 2017: 557-564.
- [34] YAN Z, ZHANG P, VASILAKOS A V. A survey on trust management for Internet of things[J]. Journal of Network and Computer Applications, 2014, 42: 120-134.
- [35] BONNEAU J, HERLEY C, VAN OORSCHOT P C, et al. The quest to replace passwords: a framework for comparative evaluation of web authentication schemes[C]//Proceedings of the 2012 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2012: 553-567.
- [36] WANG D, LI W T, WANG P. Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks[J]. IEEE Transactions on Industrial Informatics, 2018, 14(9): 4081-4092.
- [37] SYVERSON P. A taxonomy of replay attacks [cryptographic protocols[C]//Proceedings of the Computer Security Foundations Workshop VII. Piscataway: IEEE Press, 1994: 187-191.
- [38] ADKINS H. An update on attempted man-in-the-middle attacks [EB]. 2011.
- [39] SAAD M, SPAULDING J, NJILLA L, et al. Exploring the attack surface of blockchain: a comprehensive survey[J]. IEEE Communications Surveys & Tutorials, 2020, 22(3): 1977-2008.
- [40] LAURIE B. Certificate transparency[J]. Queue, 2014, 12(8): 10-19.
- [41] WEN Y H, LIU M X, YANG X W, et al. BUA: a blockchain-based unlinkable authentication scheme for mobile IoT[J]. Enterprise Information Systems, 2024, 18(2).
- [42] REBELLO G A F, CAMILO G F, DE SOUZA L A C, et al. A survey on blockchain scalability: from hardware to layer-two protocols[J]. IEEE Communications Surveys & Tutorials, 2024, 26(4): 2411-2458.
- [43] BARNES R, HOFFMAN-ANDREWS J, MCCARNEY D, et al. Automatic certificate management environment (ACME)[R]. RFC 8555, 2019.
- [44] WANG Z, LIN J Q, CAI Q W, et al. Blockchain-based certificate transparency and revocation transparency[C]//Proceedings of the Financial Cryptography and Data Security. Berlin: Springer, 2019: 144-162.
- [45] LOIBLA A, NAAB J. Namecoin [EB]. 2014.

- [46] TOORANI M, GEHRMANN C. A decentralized dynamic PKI based on blockchain[C]//Proceedings of the 36th Annual ACM Symposium on Applied Computing. New York: ACM, 2021: 1646-1655.
- [47] REN Y J, LIU X Y, WU Q, et al. Cryptographic accumulator and its application: a survey[J]. Security and Communication Networks, 2022(1): 5429195.
- [48] AL-BASSAM M. SCPKI: a smart contract-based PKI and identity system[C]//Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts. New York: ACM, 2017: 35-40.
- [49] YAKUBOV A, SHBAIR W, STATE R. BlockPGP: a blockchain-based framework for PGP key servers[C]//Proceedings of the 2018 Sixth International Symposium on Computing and Networking Workshops (CANDARW). Piscataway: IEEE Press, 2018: 316-322.
- [50] GARFINKEL S. PGP: pretty good privacy[M]. O'Reilly Media Inc, 1995.
- [51] TOMESCU A, DEVADAS S. Catena: efficient non-equivocation via Bitcoin[C]//Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2017: 393-409.
- [52] MELARA M S, BLANKSTEIN A, BONNEAU J, et al. CONIKS: Bringing Key Transparency to End Users[C]//Proceedings of the 24th USENIX Security Symposium. Washington, D C: USENIX Association, 2015: 383-398.
- [53] DONG Y H, KIM W, BOUTABA R. Conifer: centrally-managed PKI with blockchain-rooted trust[C]//Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). Piscataway: IEEE Press, 2018: 1092-1099.
- [54] YAKUBOV A, SHBAIR W M, WALLBOM A, et al. A blockchain-based PKI management framework[C]//Proceedings of the NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium. Piscataway: IEEE Press, 2018: 1-6.
- [55] KUBILAY M Y, KIRAZ M S, ALI MANTAR H. CertLedger: a new PKI model with certificate transparency based on blockchain[J]. Computers & Security, 2019, 85: 333-352.
- [56] JOSEPH ANTONY A, SINGH K. A blockchain-based public key infrastructure for IoT-based healthcare systems[J]. The Computer Journal, 2024, 67(4): 1531-1537.
- [57] AKRAM J, ANAISSI A. Decentralized PKI framework for data integrity in spatial crowdsourcing drone services[C]//Proceedings of the 2024 IEEE International Conference on Web Services (ICWS). Piscataway: IEEE Press, 2024: 643-653.
- [58] CHEN J, YAO S X, YUAN Q, et al. CertChain: public and efficient certificate audit based on blockchain for TLS connections[C]//Proceedings of the IEEE INFOCOM 2018 - IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2018: 2060-2068.
- [59] TARKOMA S, ROTHENBERG C E, LAGERSPETZ E. Theory and practice of bloom filters for distributed systems[J]. IEEE Communications Surveys & Tutorials, 2012, 14(1): 131-155.
- [60] QIN B, HUANG J K, WANG Q, et al. Cecoin: a decentralized PKI mitigating MitM attacks[J]. Future Generation Computer Systems, 2020, 107: 805-815.
- [61] FRANKLIN M K, REITER M K. Fair exchange with a semi-trusted third party[C]//Proceedings of the 4th ACM Conference on Computer and Communications Security. New York: ACM, 1997: 1-5.
- [62] FEI S F, YAN Z, WANG D L, et al. B5G-NFM: blockchain-based 5G network function management with enhanced security and privacy[J]. IEEE Transactions on Networking, 2025, 33(3): 1128-1143.
- [63] BENET J. IpfS-content addressed, versioned, P2P file system[J]. arXiv preprint arXiv:1407.3561, 2014.
- [64] LI H Z, CHEN Y J, SHI X, et al. FISCO-BCOS: an enterprise-grade permissioned blockchain system with high-performance[C]//Proceedings of the SC23: International Conference for High Performance Computing, Networking, Storage and Analysis. Piscataway: IEEE Press, 2023: 1-17.
- [65] INTERNATIONAL TELECOMMUNICATION UNION. 8th revised baseline text for X.DPKI: decentralized public key infrastructure [R]. Geneva: ITU-T, 2023.
- [66] EZUGWU A E, IKOTUN A M, OYELADE O O, et al. A comprehensive survey of clustering algorithms: State-of-the-art machine learning applications, taxonomy, challenges, and future research prospects[J]. Engineering Applications of Artificial Intelligence, 2022, 110: 104743.
- [67] KASNECI E, SESSLER K, KÜCHEMANN S, et al. ChatGPT for good? On opportunities and challenges of large language models for education[J]. Learning and Individual Differences, 2023, 103: 102274.
- [68] 李凤华, 李晖, 贾焰, 等. 隐私计算研究范畴及发展趋势[J]. 通信学报, 2016, 37(4): 1-11.
- LI F H, LI H, JIA Y, et al. Privacy computing: concept, connotation and its research trend[J]. Journal on Communications, 2016, 37(4): 1-11.
- [69] ZHANG F G, KIM K. ID-based blind signature and ring signature from pairings[C]//Proceedings of the Advances in Cryptology—ASIACRYPT 2002. Berlin: Springer, 2002: 533-547.
- [70] LIU X M, XIE H M, YAN Z, et al. A survey on blockchain sharding[J]. ISA Transactions, 2023, 141: 30-43.
- [71] GUDGEON L, MORENO-SANCHEZ P, ROOS S, et al. SoK: layer-two blockchain protocols[C]//Proceedings of the Financial Cryptography and Data Security. Cham: Springer, 2020: 201-226.

[作者简介]



史晔 (1998-), 男, 河南郑州人, 西安电子科技大学博士生, 主要研究方向为区块链、去中心化基础设施。



闫峥（1972-），女，安徽亳州人，博士，西安电子科技大学教授、博士生导师，主要研究方向为信任管理、可信AI、隐私保护、网络安全。



王海光（1973-），男，内蒙古乌拉特前旗人，博士，华为技术有限公司高级研究员，主要研究方向为5G/6G网络安全技术、可信网络、公钥基础设施证书管理。



张滋炯（2000-），男，河北石家庄人，西安电子科技大学硕士生，主要研究方向为区块链、分布式与并行计算。



李铁岩（1971-），男，天津人，博士，华为技术有限公司高级工程师，主要研究方向为网络安全、数字身份与数据空间安全。